IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application	)		
No. 10/029,639	)	**For:**	**METHOD AND APPARATUS FOR FAST CRYPTOGRAPHIC KEY GENERATION**
	)		
	)		
Mauro II, et al.	)		
	)		
Examiner: Sandoval, Kristin D.	)		
	)		
Filed: 12/19/2001	)	**Group No.**	**2132**

RESPONSE ACCOMPANYING THE FILING OF AN RCE

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

In response to the final Office Action dated May 2, 2008, please amend the above-identified application as indicated below.

ELECTRONIC FILING

Transmitted electronically to the Patent and Trademark Office.

Depositor's Name: **Tram Q. Le**
(type or print name)

Date: August 4, 2008

Signature: /Tram Q. Le/

PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

Claims 1-11 (Canceled)

12. (Currently Amended) A method for fast generation of a cryptographic key, comprising:

generating a first public key for encrypting a first wireless communication; and

generating, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

13. (Canceled)

14. (Previously Presented) The method of claim 32, further comprising:

using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

15. (Previously Presented) The method of claim 32, further comprising:

generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

16. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

means for generating a first public key for encrypting a first wireless communication; and

means for generating, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting

the second wireless communication, wherein the second public key is independent of the first public key.

17. (Canceled)

18. (Previously Presented) The wireless communication device of claim 33, further comprising:

means for using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

19. (Previously Presented) The wireless communication device of claim 33, further comprising:

means for generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

20. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for generating a first public key to encrypt a first wireless communication and generating, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication; and

a memory for storing the second public key,

wherein the second public key is independent of the first public key.

21. (Currently Amended) A processor for fast generation of a cryptographic key, said processor being configured to:

generate a first public key for encrypting a first wireless communication; and

generate, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

22. (Currently Amended) A computer program product comprising instructions for fast generation of a cryptographic key, wherein the instructions upon execution cause a computer to:

generate a first public key for encrypting a first wireless communication; and

generate, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

23. (Previously Presented) The computer program product of claim 22, wherein the instructions upon execution further cause a computer to:

determine whether the second public key has been stored prior to establishing the second wireless communication.

24. (Previously Presented) The computer program product of claim 23, wherein the instructions upon execution further cause a computer to:

use the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

25. (Previously Presented) The computer program product of claim 23, wherein the instructions upon execution further cause a computer to:

generate a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

26. (Previously Presented) The processor of claim 21, wherein said processor is further configured to:

determine whether the second public key has been stored prior to establishing the second wireless communication.

27. (Previously Presented) The processor of claim 26, wherein said processor is further configured to:

use the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

28. (Previously Presented) The processor of claim 26, wherein said processor is further configured to:

generate a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

29. (Previously Presented) The wireless communication device of claim 20, wherein the processor determines whether the second public key has been stored prior to establishing the second wireless communication.

30. (Previously Presented) The wireless communication device of claim 29, wherein the processor uses the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

31. (Previously Presented) The wireless communication device of claim 29, wherein the processor generates a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

32. (Previously Presented) The method of claim 12, further comprising:

determining whether the second public key has been stored prior to establishing the second wireless communication.

33. (Previously Presented) The wireless communication device of claim 16, further comprising:

means for determining whether the second public key has been stored prior to establishing the second wireless communication.

34. (New) A method for fast generation of a cryptographic key, comprising:

generating a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

35. (New) The method of claim 34, further comprising:

generating a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

36. (New) A wireless communication device for fast generation of a cryptographic key, comprising:

means for generating a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

means for generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

37. (New) The wireless communication device of claim 36, further comprising:

means for generating a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

38. (New) A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for:

generating a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication, and

generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication; and

a memory for storing the second public key and the corresponding second key, wherein the second public key is independent of the first public.

39. (New) The wireless communication device of claim 38, wherein the processor generates a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

40. (New) A processor for fast generation of a cryptographic key, said processor being configured to:

generate a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

generate, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

41. (New) The processor of claim 26, wherein said processor is further configured to:

generate a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

42. (New) A computer program product comprising instructions for fast generation of a cryptographic key, wherein the instructions upon execution cause a computer to:

generate a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

generate, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

43. (New) The computer program product of claim 42, wherein the instructions upon execution further cause a computer to:

generate a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

REMARKS

Claims 12, 14-16 and 18-43 are pending in the present application. In the above amendments, claims 12, 16 and 20-22 have been amended, and new claims 34-43 have been added.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 103

The Examiner rejected claims 12, 14-16 and 18-33 under 35 U.S.C. §103(a) as being allegedly unpatentable over over Dierks et al., The TLS Protocol, Version 1.0 (the Dierks publication) in view of U.S. Patent No. 7,237,261 to Huber et al. (the Huber patent), and further in view of U.S. Patent No. 6,955,299 to Pathmasuntharan et al. (the Pathmasuntharan patent).

The rejection of claim 12 as being unpatentable over the Dierks publication in view of the Huber patent and further in view of the Pathmasuntharan patent, is respectfully traversed. Claim 12, as amended, recites a "method for fast generation of a cryptographic key, comprising: generating a first public key for encrypting a first wireless communication; and generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key." Support for the amendment to claim 12 is in the original specification in paragraphs [0021] through [0022], and in Figure 2, steps 202-204. The Dierks publication fails to disclose or suggest, "generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key," as recited in claim 12, and the Huber patent fails to remedy the disclosure deficiencies of the Dierks publication. The newly cited Pathmasuntharan patent discloses generating a transaction key, and communicates the generated transaction key to an enabler device before terminating a communication with the enabler device. See, column 13, lines 39-49, and Figure 8, reference points 6 and 7. Thus, the Pathmasuntharan patent teaches generating a transaction key before termination of a communication with the enabler device. Further, the transaction key is merely a random number which is stored by a smart card and an enabler device for comparison at the next transaction.

See, column 9, lines 7-12, column 11, lines 10-40, and column 12, lines 2-6. Applicants assert there is no disclosure or suggestion that the transaction key of the Pathmasuntharan patent is used for encrypting a second wireless communication. Therefore, since the Dierks publication, the Huber patent, and the Pathmasuntharan patent, do not disclose or suggest all of the recited features, Applicants respectfully request the Examiner to withdraw the rejection of claim 12.

It is respectfully submitted that dependent claims 14-15 and 32 are at least allowable for the reasons given above in relation to independent claim 12.

Claims 16-31 and 33 are wireless communication device, processor, and computer program product claims having features defined by language similar to that of method claims 12, 14-15 and 32. It is respectfully submitted that claims 16-31 and 33 are at least allowable for the reasons given above in relation to claims 12, 14-15 and 32.

New Claims

Support for new claims 34-43 may be located in the original specification at paragraphs [0019] – [0024]. Applicants respectfully asserts that new claims 34-43 recite patentable matter as discussed above with respect to claims 12-33, and for recitation of first and second private keys and first and second shared keys.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **August 4, 2008**

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502